

Plane recovery goes on

By 2d Lt Jeffrey Bishop
18th Wing Public Affairs

KADENA AIR BASE, Japan (AFPN) – Kadena people are playing a key role in the recovery of the EP-3 surveillance plane from Hainan Island, China.

Employees of Lockheed Martin Aeronautics Co., the contractor hired by the Defense Department to take the plane apart and bring it back to the United States, left here June 20 for China. They will be continuing work on the Navy plane that made news when it was forced to make an emergency landing at Lingshui Airfield on April 1 after a Chinese interceptor collided with it in flight.

Parts from the plane will be ferried to Kadena in a series of shipments on a contracted Russian AN-124 commercial cargo jet. The large-capacity aircraft, operated by Polyot Air Cargo Ltd., of Voronezh, Russia, is comparable to a C-5 Galaxy.

While Kadena personnel will not go to China to participate in the aircraft's recovery, they are lending support to the contracted crews. About 60 people will be directly involved, with many more people providing indirect support.

The operation is expected to take a few weeks to accomplish.



Photo by A1C Harold Barnes III

Who's in your chain of command?

Amn Aaron Roberts, TSgt Ruth Arsenault and A1C Carlos Litsinger, 341st Mission Support Squadron, stand in front of the recently established chain-of-command wall. The display shows 341st MSS members their squadron commander, Lt Col Ashley Elder, to President George W. Bush.

Big Brother's watching

DOD agents continue chasing hackers

By Steve Hara
American Forces Press Service

WASHINGTON (AFPN) – Defense Department computer security systems and specialists foiled nearly 22,500 would-be intruders in 1999, and 24,500 in 2000. There is no let-up in sight.

Special Agent Jim Christy said he and others on his law enforcement staff are in a growth business, chasing hackers and spies and running down other criminal activities. As representatives of the office of the assistant secretary of defense for command, control, communications and intelligence, they also counsel DOD employees on being an effective first line of defense instead of the weakest link.

When he discusses computer security, Christy said, he drives home that average folks are not expected to mount an ironclad defense. Rather, he stressed, they can do simple things that make life harder for bad guys – and can stop doing simple things

that make life easier for them.

Here are some simple things that can help:

- Use different passwords at Web sites and on every machine you use. Reject all site and system offers to "remember" a person and his password. Bad guys know many people use just one password, so attacking an easily hacked site gives them "skeleton keys" to tough ones.

- Do not open e-mail attachments from people you do not know, and do not open them uncritically just because someone known supposedly sent them. Hackers use attachments to inject viruses and other mischievous or malicious computer code into machines and systems. A common means to spread infections is by sending e-mail copies to everyone in a victim's address book – using the victim's name.

- Log off or lock a workstation when you go on breaks or out to lunch. There is no point giving bad guys unfettered access to a computer and network.

- Never use personal diskettes, Zip disks and the like on classified systems. Computers divide files and write them to disk in units called sectors. If the file's last sector is only partially filled, the machine tops it off with data

randomly pulled from memory or hard drives. There is no way to know in advance where the information might come from, so writing and saving even your holiday greetings letter on a classified system is considered a security violation.

- People can be a security risk even if they do not work with classified files, have none on your computer and have no access to any. Hackers can launch network attacks from unclassified computer systems, given the time and opportunity. And intelligence analysts are quite capable of drawing conclusions from bits and pieces of unclassified, seemingly unrelated information.

Keep in mind that information does not have to be classified to be sensitive, Christy said. Medical records, personnel records and personal address and telephone books are not usually classified, but all contain data protected from public release by the Privacy Act of 1974. Good security, he said, means locking out all snoopers, not just spies.

Christy and company's growing business in security issues gives rise to another – personal privacy on government-owned computers. Government users have none.

Uncle Sam's machine, Uncle Sam's rules, Christy noted.

"There is absolutely no privacy on a government computer," Christy said.

"There's absolutely no privacy on a government computer."

Jim Christy
Special agent

AFA conference brings space 'stars' together

One-day conference held ideas, support for U.S. space control

By MSgt Austin Carter
AFSPC Public Affairs

COLORADO SPRINGS, Colo. – The "stars" of military and industrial space gathered for an annual Air Force Association conference recently to discuss the future of space operations for the United States.

In a one-day conference held last month at the Broadmoor Hotel in Colorado

Springs leaders of the aerospace industry mingled with servicemembers who make sure the United States maintains its superiority in space.

The conference began with a panel of 12 stars: three major command commanders, all with different perspectives of space. Gen Ed Eberhart, commander of Air Force Space Command and commander in chief of U.S. Space Command and North American Aerospace Defense Command; Gen John Jumper, commander of Air Combat Command and Gen Lester Lyles, commander of Air Force Materiel Command, each spoke of a renewed focus on the use of space capabilities in the military.

Gen Eberhart likened that renewed interest to the race to the moon in the 1960s. However, he urged a new direction.

"We must think beyond force enhancement," Gen Eberhart stated. "We must think now of space control."

Space control is considered by military strategists to be the ability to protect and defend space assets and deny the use of space to an enemy.

"We must use space to attack the center of gravity of our adversaries," he said. "We must control space as we would attempt to control land, sea and air."

Gen Jumper, as one of the prime customers of AFSPC's products, reminded the audience that America will need to create a

"warrior class" to operate military space systems in future conflicts. He said the military must create a new environment by tearing down the inter- and intraservice boundaries so that the warrior can get timely information for his mission. Gen Lyles, whose command handles the acquisition processes and product development for the rest of the Air Force, handled questions about the upcoming merger of Space and Missile Systems Center and AFSPC Oct. 1.

"I'm telling our people not to look at it as a developmental organization turning into an operational command," he said. "We're creating a new culture here, not wholly ops or developmental. Space and air integration is absolutely critical."